Accellion Share Securely™

AN ACCELLION WHITE PAPER

Secure File Sharing for HIPAA Compliance: Protecting PHI

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

WP-HIPAA-112

Executive Summary

Healthcare organizations (HCOs) and their partners make themselves vulnerable to data breaches by transferring confidential files through physical media such as CDs and USB sticks and over online channels such as FTP or email. Physical media can be lost or stolen. Files transmitted by FTP or email can be intercepted or copied. The sheer number of data breaches involving Protected Health Information (PHI)—166 major data breaches were reported to the U.S. Department of Health and Human Services in 2010—demonstrates that HCOs do not have adequate data security controls in place.

166 major data breaches were reported to the Department of Health and Human Services in 2010.

While HCOs struggle to contain these risks, data security regulations are becoming increasingly strict. Recent federal regulations have updated HIPAA and introduced new FTC rules mandating tighter security for HCOs and their partners. Many states are passing data breach notification laws, requiring HCOs to disclose data security lapses and increasing the risk of civil lawsuits and tarnished brands.

To address the security problems inherent in consumer-grade file sharing apps, email, and other risky technologies, HCOs and their partners should implement an easy-to-use, enterprise-wide secure file sharing solution. A secure file sharing and collaboration solution complements other communication tools such as email, while ensuring that PHI is delivered over a separate secure, auditable channel. Users can securely send files to other authorized users. Data is encrypted for protection. Security controls prevent files from being forwarded to unauthorized users. All file access is monitored and logged.

By implementing a secure file sharing solution, HCOs reduce the risk of data breaches and improve their compliance with industry regulations such as HIPAA.

.

Introduction

Is anyone in your organization still using CDs, FTP, or USB sticks to transfer Protected Health Information (PHI)? If so, your organization is at risk for non-compliance with the Health Insurance Portability and Accountability Act (HIPAA). Your organization is also running the risk of a serious data breach, making news headlines, and incurring hefty regulatory fines.

As a cautionary tale, consider the case of a doctor at NYU Langone Medical Center who used an unencrypted USB stick to store the PHI of 2,563 patients undergoing procedures at the clinic. The data included names, ages, genders, medical record numbers, and descriptions of medical procedures. When the USB stick was discovered missing in May 2010, the medical center was forced to notify patients and the public of its data breach.[1] Many organizations that disclose breaches like this soon find themselves the subjects of civil lawsuits.

Nearly a quarter of healthcare organization CIOs reported suffering a security breach in the previous 12 months.

NYU got off pretty lightly, all considered. The pharmaceutical giant Rite Aid is paying a steeper price for its own PHI security breach. Rite Aid employees were caught disposing of prescription information in trash cans outside Rite Aid stores. The Office of Civil Rights (OCR) in the Department of Health and Human Services (HHS) concluded that this behavior violated HIPAA regulations. For this indiscretion, the OCR fined Rite Aid $1 million.[2]

PHI data breaches are all too common. In the past year alone, the HHS was notified of 166 major data breaches, each affecting at least 500 patients, and affecting 4.9 million PHI data sets in total.[3] Nearly a quarter of healthcare organization CIOs reported suffering a security breach in the previous 12 months.[4] Some of these breaches involved USB sticks or stolen laptops. Others involved careless email messages or unprotected servers. All of them put healthcare organizations (HCOs) at risk of financial penalties, tarnished brands, and lost business.

[1] http://www.phiprivacy.net/?p=3108

[2] http://www.hhs.gov/news/press/2010pres/07/20100727a.html

[3] http://www.docehrtalk.org/messageboard/2010/10/01/hhs-presents-major-data-breaches-line

[4] The 2010 HIMSS (Healthcare Information and Management Systems Society) Leadership Survey, http://www.himss.org/2010Survey/

HCOs and their partners need to recognize the substantial, but avoidable risks of transferring files through physical media such as CDs or USB sticks, or over online channels such as FTP or email. HCOs also need to be aware of the increasingly strict regulations governing PHI and data breaches. While HCOs continue to struggle with IT controls for preventing PHI data breaches, regulators are tightening controls and making penalties steeper than ever before.

New Data Breach Laws and Regulations

HIPAA: Tougher Enforcement and Higher Fines through the HITECH Act

HCOs are generally familiar with HIPAA by now, but they might not be as familiar with recent changes to HIPAA that have been enacted in 2009 and 2010.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA), broadens the scope of HIPAA to cover business partners of HCOs. This means that communications with business partners such as accountants and consultants are now subject to HIPAA security controls.

The HITECH Act also moves HIPAA enforcement to the Office of Civil Rights within the HHS, increases the upper limits on fines,[5] and gives regulators a new incentive for enforcing penalties: payments for fines go straight into the departmental budgets of the regulators.

As the $1 million fine imposed on Rite Aid shows, the OCR intends to enforce HIPAA rigorously.[6]

In addition to HIPAA regulations, there are other federal and state laws that HCOs should consider when evaluating the risks of data security breaches.

FTC Rules

The FTC has its own healthcare rules related to data security.

The FTC's Healthcare Breach Law, which took effect February 22, 2010, requires certain businesses not covered by HIPAA to notify customers and others if PHI is exposed. The law is designed to cover sites that manage patient health records but that are not providers or insurers.

The FTC's Red Flags Rule, which took effect August 1, 2009, requires "certain businesses and organizations — including many doctors' offices, hospitals, and other health care providers — to develop a written program to spot the warning signs — or 'red flags' — of identity theft." Failure to develop a program to spot red flags can result in a fine.[7]

[5] http://www.hhs.gov/news/press/2009pres/10/20091030a.html

[6] http://www.scmagazineus.com/rite-aid-to-pay-1-million-fine-for-hipaa-violation/printarticle/175729/

[7] "The 'Red Flags' Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft," http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm

Data Breach Notification Laws

As of this writing, 46 states, the District of Columbia, and Puerto Rico have enacted data breach notification laws.[8] Data breach notification laws require HCOs and other organizations to notify the public when confidential data has been exposed. Requirements for notifications vary from state to state. States such as California and Massachusetts require companies to issue notifications even if only a single resident's data was exposed in a data breach. Other states require notifications only if hundreds or thousands of residents were affected. In Missouri, for example, companies are required to report breaches only if records for 1,000 or more people were exposed.

Who receives these notifications? That, too, varies from state to state. Typically, an HCO must notify all members of the public whose records were exposed. But HCOs might also have to notify a state agency in charge of consumer protection, the state Attorney General, and national consumer protection agencies.

Upon learning of a data breach, 6% of healthcare customers severed their relationship with the HCO responsible for the breach.

Data breach notifications have broad ramifications for HCOs. They can lead to criminal and civil investigations. They can increase the costs of handling data breaches—costs that on average reached $6.75 million per incident in the U.S. in 2009.[9] They can tarnish a company's brand irrevocably. They can lead to lost business. Upon learning of a data breach, 6% of healthcare customers severed their relationship with the HCO responsible for the breach.[10]

File Sharing and Data Breaches

Given the increased penalties HCOs are facing for HIPAA violations, best practices dictate that HCOs audit their IT practices and identify likely causes of data security breaches.

File transfers are likely culprits. PHI circulates continually within an HCO and among HCOs. Medical records move from one doctor to another, from one clinic to another, from a hospital to insurers, and so on. It's natural for care-givers and other HCO employees to transfer PHI the same way they transfer their other files. They use email, USB sticks, or FTP servers, trusting that these technologies are secure.

Unfortunately, they're not. All these technologies suffer from security vulnerabilities that jeopardize the security of PHI.

- USB memory sticks can be lost or stolen.
- Email can be intercepted, forwarded to unauthorized users, or inadvertently sent to the wrong recipient.
- FTP severs are often used to store confidential files, but the files are often forgotten or access is not secure.
- IM users usually transfer files without encryption and to recipients whose IDs can easily be spoofed.
- Courier services can lead to physical media such as tapes and CDs being lost, stolen, or damaged.
- Free file-sharing services can put vital communications outside the purview of the IT department and leak data to untrusted third parties

[8] http://www.ncsl.org/default.aspx?tabid=13489
[9] http://www.ponemon.org/news-2/23
[10] http://www.ponemon.org/news-2/23

News stories abound about lost USB sticks, lost backup tapes and CDs, and other data security mishaps that result in damaging data breaches.[11] These stories keep appearing because even with the best intentions, HCOs cannot make these technologies secure enough to protect PHI.

The Solution: Secure File Sharing

Fortunately, there is an easy way to address the security problems inherent in email, FTP, and other risky technologies: implement an easy-to-use, enterprise-wide secure file sharing solution. A secure file sharing solution complements other communication tools such as email, while ensuring that PHI is delivered over a separate secure, auditable channel. Users can securely share files with other authorized users. Data is encrypted for protection. Security controls prevent files from being forwarded to unauthorized users. All file access is monitored and logged.

Once a secure file transfer solution is in place, HCO employees no longer have to rely on FTP, P2P, data sticks, and other unsecure channels for transferring files.

Once a secure file sharing solution is in place, HCO employees no longer have to rely on FTP, P2P, data sticks, and other unsecure channels for transferring files. The IT department can manage and audit file transfers, ensuring that users are complying with security policies. And IT managers and compliance officers can breathe a sigh of relief now that they have secured countless file transfers that otherwise would have jeopardized the HCO's compliance with HIPAA and other regulations.

The Accellion Solution for Secure File Sharing

Accellion provides enterprise-class mobile file sharing solutions that enable secure anytime, anywhere access to information while ensuring enterprise security and compliance. Leading HCOs, as well as other leading corporations and government agencies, rely on Accellion file sharing solutions to securely send confidential data and ensure compliance with industry regulations. Accellion provides organizations with flexible, scalable deployment options that can grow from a single office to globally distributed deployment integrating public, and private cloud installations.

With Accellion Secure Collaboration, HCOs can protect the transfer of PHI and intellectual property, reduce security exposure, ensure compliance, improve email performance, replace non-secure FTP, and reduce IT support, all while providing care-givers and administrators an easy-to-use mobile solution that works with the email and IM programs they already know.

Key Benefits of Accellion Secure File Sharing

- Provides secure mobile file sharing of Enterprise content to internal and external recipients
- Enables real-time collaboration with colleagues, partners, customers, and vendors
- Reduces risk of data breaches
- Increases data security

[11] For example, here's a story about a lost USB stick containing health records of patients at a secured mental health hospital: http://www.theregister.co.uk/2010/05/05/mental_hospital_usb_stick/

- Provides file tracking and reporting tools to demonstrate compliance with HIPAA, SOX, GLBA
- Increases business productivity and reduces business cycle time
- Improves email performance and reduces email storage by offloading files
- Replaces unsecure FTP
- Reduces IT support

The Accellion Secure File Sharing solution is already in use at leading healthcare facilities such as Beth Israel Deaconess Medical Center and Cornell University Weill Medical College.

Beth Israel Deaconess Medical Center

Beth Israel Deaconess Medical Center (BIDMC), one of the top-ranked hospitals in the U.S., relies heavily on its email system to quickly share information among staffers and outside researchers. Several years ago, the hospital's IT department recognized that email posed a substantial risk to PHI data security. Imposing stricter email policies simply led employees to find dangerous work-arounds. The IT team tried building their own secure file transfer system, but the costs turned out to be prohibitive. Meanwhile, the IT team was getting daily calls, asking for help transferring large files.

Click here to read the BIDMC case study and learn why BIDMC selected Accellion to meet its secure file transfer requirements.

Indiana University Health

Indiana University Health, a premier provider of health care in the U.S. Midwest, runs a telemedicine program that services thousands of patients in an area covering hundreds of square miles. The program depends on caregivers being able to send and receive critical medical data, including files as large as 100 MB, to patients at remote locations. But relying on email for this communication is problematic: many email servers reject attachments larger than 10 MB, and email is not necessarily secure enough to comply with HIPAA.

To learn why Indiana University Health selected Accellion to deliver files quickly and securely to remote caregivers, click here to read the case study.

Conclusion

Don't risk HIPAA regulatory penalties, lost business, and other damages from data breaches. Protect PHI with Accellion. You'll minimize the risks of data security breaches while also reducing the IT overhead associated with less secure file-sharing technologies such as Dropbox-type applications, FTP and CDs. Best of all, you'll give caregivers prompt, secure access to the information they need in order to deliver the best possible medical care.

About Accellion, Inc.

Accellion provides enterprise-class mobile file sharing solutions that enable secure anytime, anywhere access to information while ensuring enterprise security and compliance. The world's leading corporations and government agencies use Accellion to protect intellectual property, ensure compliance, improve business productivity and reduce IT costs. Founded in 1999, Accellion file sharing solutions can be deployed on public, private and hybrid cloud environments and provide the ease-of-use business users need while giving the enterprise organization the flexibility, scalability and protection it needs. For more information please visit www.accellion.com or call (650)-485-4300. Follow Accellion's Blog, Twitter, Facebook, and LinkedIn.

www.accellion.com

info@accellion.com

THIS DOCUMENT IS PROVIDED "AS IS." ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.